WHAT IS CLAIMED IS:

1. A security method for use in a communication system, the security method comprising:

receiving an IP packet including a source address and a destination address;

obtaining physical location information indicating the location of a user device which is the source of said IP packet; and

determining, as a function of the obtained physical location information, an action to be taken.

2. The security method of claim 1, wherein determining an action to be taken includes:

comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided.

3. The security method of claim 2, further comprising:

dropping said packet when said comparing does not result in a match between the obtained physical location information and the information listing physical locations authorized to obtain access to the service.

4. The security method of claim 2, wherein said service is one of a banking service, video on demand service and a music on demand service.

5. The security method of claim 2, further comprising:

forwarding said packet to the destination address when said comparing results in a match between the obtained physical location information and the information listing physical locations authorized to obtain access to the service.

6. The security method of claim 1, wherein obtaining physical location information includes:

transmitting a location information request message including the source address of the received IP packet; and

receiving in response to said transmitted location information request message, information corresponding to the location of the user device.

7. The security method of claim 6, further comprising:

determining the location of the user device from edge router and port information obtained from an edge router.

8. The security method of claim 7, wherein determining the location of the user device further includes:

performing a database lookup operation to retrieve a geographic location stored in association with said edge router and port information.

9. The security method of claim 8, further comprising:

further receiving, in response to said transmitted location information request message, a device identifier associated with the source address of said IP packet; and

comparing the received device identifier to a list device identifiers corresponding to stolen devices.

10. The security method of claim 9, wherein said device identifier is a MAC address.

11. The method of claim 9, further comprising:

generating a message indicating the detection of a stolen device when said comparing step detects a match between the received device identifier and an device identifier in said list of device identifiers corresponding to stolen devices.

12. The method of claim 11, wherein said generated message includes information indicating the a geographic location where the identified stolen device is being used.

13. The method of claim 12, wherein said geographic location is a post office address.

14 The method of claim 1, further comprising:

determining if the destination address corresponds to a service for which security is to be provided; and

wherein said steps of obtaining physical location information and determining an action to be taken are performed when it is determined that said destination address corresponds to a service for which security is to be provided.

15. A security device for use in a communication system in which IP packets are transmitted, the device comprising:

means for receiving an IP packet including a source address and a destination address;

means for obtaining physical location information indicating the location of a user device which is the source of said IP packet; and

means for determining, as a function of the obtained physical location information, an action to be taken.

16. The security device of claim 15, further comprising:

a database of physical location information listing physical locations authorized to obtain access to said service; and

wherein said means for determining an action to be taken includes a comparator for comparing the obtained physical location information to information listing physical locations authorized to obtain access to a service for which security is to be provided.

17. The security device of claim 16, further comprising:

means for dropping said packet when said comparing does not result in a match between the obtained physical location information and the information listing physical locations authorized to obtain access to the service.

18. The security device of claim 2, wherein said service is one of a banking service, video on demand service and a music on demand service.

19. A stolen device detection method, the method comprising the steps of:

storing a list of device identifiers corresponding to stolen devices;

receiving an IP packet from a device including an IP address associated with said device;

using said IP address associated with said device to determine a device identifier also associated with said device;

comparing the determined device identifier to said stored list of device identifiers corresponding to stolen devices; and

determining that said IP address corresponds to a stolen device when said determined device identifier matches a device identifier in said stored list.

20. The stolen device detection method of claim 19, wherein said determined device identifier is a MAC address and wherein said stored list of device identifiers is a list of MAC addresses.

21. The stolen device detection method of claim 19, further comprising:

determining the location from which said device is used from said IP address and from information determined from a MAC address corresponding to said device.

22. The stolen device detection method of claim 21, further comprising:

generating a message indicating the location of device determined to be a stolen device, said message including the determined location form which said device is being used.

23. The stolen device detection method of claim 21, wherein said step of determining the location from which said device is used includes:

determining a router and port through which said device transmitted said IP packet; and

obtaining location information from a database associating router and port numbers with physical locations corresponding to subscriber premises.

24. The stolen device detection method of claim 23, further comprising:

storing owner contact information with said list of stolen device identifiers.

25. The stolen device detection method of claim 24, wherein said owner contact information includes an E-mail address corresponding to an owner of a stolen device.

26. The stolen device detection method of claim 23, further comprising:

storing law enforcement contact information with said list of stolen device identifiers.

27. The stolen device detection method of claim 24, wherein said law enforcement contact information includes an E-mail address corresponding to an owner of a stolen device.

28. A system for detecting stolen devices using IP addresses, the system comprising:

a stored list of device identifiers corresponding to stolen devices;

means for receiving an IP packet from a device including an IP address associated with said device;

means for determining a device identifier associated with said device from said IP address associated with said device;

means for comparing the determined device identifier to said stored list of device identifiers corresponding to stolen devices; and

means for determining that said IP address corresponds to a stolen device when said determined device identifier matches a device identifier in said stored list.

29. The system of claim 28, wherein said determined device identifier is a MAC address and wherein said stored list of device identifiers is a list of MAC addresses.

30. The system of claim 29, further comprising:

means for determining the location from which said device is used from said IP address and from information determined from a MAC address corresponding to said device.

31. The system of claim 30, further comprising:

means for generating a message indicating the location of device determined to be a stolen device, said message including the determined location form which said device is being used.

32. A location verification method, the method comprising;

receiving an IP packet including a source address;

determining from said source address the geographic location from which said IP packet was sent;

comparing the determined geographic location information to expected information indicating the expected source of an IP packet; and

determining a reporting error when said determined geographic location information does not match the expected geographic location information.

33. The location verification method of claim 32, further comprising:

transmitting a message including information on the determined reporting error to a law enforcement authority.

34. The location verification method of claim 33, further comprising:

including the determined geographic location information in said message.

35. The location verification method of claim 34, further comprising:

identifying the device transmitting said IP packet from a MAC address determined from a database associating said MAC address with said source address.

36. The location verification method of claim 35, wherein said IP packet is transmitted from a bracelet worn by a parolee and wherein said IP packet includes parolee identification information, the method further comprising:

including in said message information obtained from said IP packet identifying the parolee.

37. The location verification method of claim 33, further comprising:

determining if said IP packet was sent at a predetermined time during which a location reporting message was scheduled to be transmitted.